

AD-A055 603

MITRE CORP BEDFORD MASS
REVISION OF DOD ADP SECURITY DIRECTIVES (U)
JUN 78 K T MAHONEY

F/G 9/2

UNCLASSIFIED

MTR-3461

ESD-TR-78-118

F19628-77-C-0001

NL

| OF |
ADA
055603



END
DATE
FILMED
8-78
DDC

FOR FURTHER TRAN *FILE*

(12)

MTR-3461

ESD-TR-78-118

AD A 055603

REVISION OF DoD ADP SECURITY DIRECTIVES

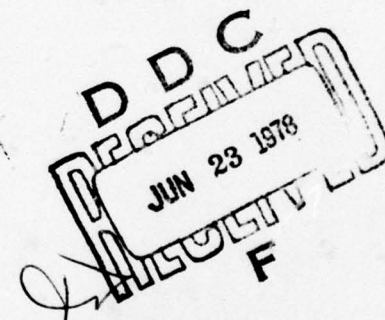
BY K. T. MAHONEY

JUNE 1978

Prepared for

DEPUTY FOR TECHNICAL OPERATIONS

ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Hanscom Air Force Base, Massachusetts



Project No. 572N

Prepared by

THE MITRE CORPORATION

Bedford, Massachusetts

Contract No. F19628-77-C-0001

Approved for public release; distribution unlimited.

78 06 21 040

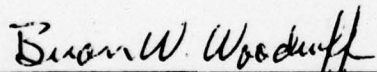
AD No. _____
DDC FILE COPY

When U.S. Government drawings, specifications, or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

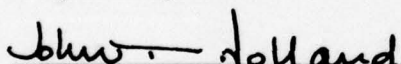
Do not return this copy. Retain or destroy.

REVIEW AND APPROVAL


This technical report has been reviewed and is approved for publication.


BRIAN W. WOODRUFF, Captain, USAF
Project Engineer


DONALD P. ERIKSEN
Project Engineer


JOHN T. HOLLAND, Lt Colonel, USAF
Chief, Techniques Engineering Division

FOR THE COMMANDER


STANLEY P. DERESKA, Colonel, USAF
Chief, Computer Systems Engineering
Deputy for Technical Operations

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

19 REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM	
1. REPORT NUMBER ESD-TR-78-118	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle) REVISION OF DoD ADP SECURITY DIRECTIVES		5. TYPE OF REPORT & PERIOD COVERED	
7. AUTHOR(s) K. T. /Mahoney		6. PERFORMING ORG. REPORT NUMBER MTR-3461	
9. PERFORMING ORGANIZATION NAME AND ADDRESS The MITRE Corp. Box 208 Bedford, MA 01730		8. CONTRACT OR GRANT NUMBER(s) F19628-77-C-0001	
11. CONTROLLING OFFICE NAME AND ADDRESS Deputy for Technical Operations Electronic Systems Division, AFSC Hanscom Air Force Base, MA 01731		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Project No. 572N	
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) 11 Jun 78		12. REPORT DATE JUNE 1978	
13. NUMBER OF PAGES 36		15. SECURITY CLASS. (of this report) UNCLASSIFIED	
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE	
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)			
18. SUPPLEMENTARY NOTES			
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) ADP SECURITY SECURITY KERNEL TECHNOLOGY INFORMATION SECURITY SECURITY POLICY MULTILEVEL SECURITY			
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This report examines three existing DoD ADP security directives (DoD 5200.28, DoD 5200.28M, and AFR 300-8) for completeness in light of the computer security technology advances made in recent years. Additions and modifications that would update the directives are presented, including suitable word changes to implement the directives' revisions.			

DD FORM 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

235 050

JOB

ACKNOWLEDGMENTS

This report has been prepared by The MITRE Corporation under Project No. 572N. The contract is sponsored by the Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Massachusetts.

The author wishes to acknowledge the suggestions provided by D. W. Snow in the areas of design and production controls, and the general access and special access properties.

ACCESSION for	
NTIS	White Section <input checked="" type="checkbox"/>
DDC	Buff Section <input type="checkbox"/>
UNANNOUNCED	
JUSTIFICATION	
BY	
DISTRIBUTION/AVAILABILITY CODES	
1	SPECIAL
A	

TABLE OF CONTENTS

	<u>Page</u>
SECTION I INTRODUCTION	5
SECTION II SECURITY POLICY IN ADP SYSTEMS	6
SECURITY POLICY	6
CURRENT ADP SECURITY PRACTICE	8
COMPUTER SECURITY REQUIREMENTS	8
Cost Impacts	9
Operational Impacts	9
MULTILEVEL SECURITY IN ADP SYSTEMS	10
TECHNICAL APPROACH TO MULTILEVEL SECURITY	11
Reference Monitor	12
Abstract Model of a Secure System	14
Formal Specification	14
Algorithmic Representation	14
Machine Language Representation	15
Verification Techniques	15
Summary	16
EXPERIENCES IN SECURE COMPUTER SYSTEMS	17
ESD/MITRE PDP-11/45 Security Kernel	17
AFDSC Secure MULTICS	18
SATIN-IV	19
AUTODIN-II	19
Secure UNIX Procurement	19
SUMMARY OF REQUIREMENTS	21
SECTION III ADDITIONS AND MODIFICATIONS TO EXISTING DIRECTIVES	23
GENERAL	23
DOD DIRECTIVE 5200.28	23
DOD MANUAL 5200.28M	24
AIR FORCE REGULATION 300-8	26

TABLE OF CONTENTS (Concluded)

	<u>Page</u>
SECTION IV CONCLUSIONS AND RECOMMENDATIONS	28
APPENDIX I PROPOSED CHANGES TO DOD 5200.28	29
SECTION I - PURPOSE	29
SECTION III - DEFINITIONS	29
SECTION IV - POLICY	29
SECTION V - RESPONSIBILITIES	30
SECTION VI - MINIMUM REQUIREMENTS	30
ENCLOSURE 2 - DEFINITIONS	30
APPENDIX II PROPOSED CHANGES TO DOD 5200.28M	31
SECTION I - GENERAL PROVISIONS	31
Part 1 - Introduction	31
SECTION II - PERSONNEL SECURITY	31
Part 1 - Clearance and Access Controls	31
SECTION IV - HARDWARE/SOFTWARE FEATURES	31
Part 1 - General	31
Part 2 - Hardware	32
Part 3 - Software	32
SECTION IX - SECURITY TESTING AND EVALUATIONS (ST&E)	32
APPENDIX III PROPOSED CHANGES TO AFR 300-8	33
PART 3 - PARAGRAPH C	33
PART 4 - INTRODUCTION	33
PART 4 - PARAGRAPH H	33
PART 6 - PARAGRAPH A	34
REFERENCES	35

SECTION I

INTRODUCTION

This paper discusses recent developments in the field of computer security technology and how these developments can be incorporated into existing ADP directives. It is important to note that, while the complete security of a system is dependent on the factors of many areas (physical, emanations, communications), this paper treats only the area of hardware/software controls in an ADP system. Toward this end, the paper consists of three main sections: Security Policy in ADP Systems, Additions and Modifications to Existing Directives, and Conclusions and Recommendations.

In the Security Policy in ADP Systems section, topics discussed include DoD security policy, security practice in current ADP systems, the multilevel security problem, and examples of multilevel secure systems. Based on the discussion, areas are identified where the directives must be changed to reflect the advances in computer security technology.

The Additions and Modifications to Existing Directives section identifies the additions necessary for the following: DoD Directive 5200.28, DoD Manual 5200.28M, and Air Force Regulation 300-8.

Lastly, the Conclusions and Recommendations section suggests the action to be taken in light of the discussion presented.

The goals of this paper are to show how computer security technology has advanced, and to show how the appropriate directives and regulations could be changed to reflect these advances. It is interesting to note that DoD 5200.28 states the necessity to upgrade the security measures put forth in the regulations when "experience and new techniques are acquired under actual operating conditions or as a result of follow-on testing and evaluation procedures."

SECTION II

SECURITY POLICY IN ADP SYSTEMS

This section discusses DoD security policy and its implementation in ADP systems. The policy is reviewed for both the paper environment and ADP systems. Current ADP security practices and the development of multilevel secure systems are discussed. Examples of systems operating in a multilevel secure mode are presented, as well as the application of computer security technology to the development of future DoD systems. A summary of the major features of computer security technology, and their impact on the existing DoD directives, is also included.

SECURITY POLICY

Security policy in an ADP system is drawn from the policy applicable to the paper environment (1), but with certain additions to reflect the added dimension of computer processing of classified information.

Security policy states that official material shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned. Classified material may be used, held, or stored only where there are facilities or conditions adequate to prevent unauthorized persons from gaining access to it. Any security requirements necessary to protect classified information must not be so restrictive as to prevent the accomplishment of essential functions.

An ADP security policy defines the access attributes of subjects and objects. (The notion of subjects and objects, when dealing with ADP system security, was first presented in (2).) A subject is defined as an active system element that is capable of requesting access to information; in the paper environment, a person can be considered as a subject, while in the ADP environment, a program or process running on behalf of a user would be considered as a subject. An object is defined as a repository of information. In the paper environment, objects would be classified documents or information; in the ADP environment, objects would be data or files.

Two security properties exist that must be satisfied in both the paper and ADP environments. The first property requires that a subject shall not be permitted to read an object of a higher classification than it is cleared to access. In the paper

environment, a person is not permitted to read classified information unless he is cleared to at least the security classification of the information. In the ADP environment, a subject (i.e., a process) at one classification cannot access data or files at a higher classification.

The second property forbids a subject from taking information of one classification and rewriting it at a lower classification. This property points out the difference between the paper and ADP environments. In the paper environment, a person is acting on his own behalf when accessing classified information. Each person is considered a trusted subject, and, as such, the person is trusted not to disclose any classified information to persons who are not suitably cleared. On the other hand, in the ADP environment, a person is not directly accessing any classified information; that is, an executing program or process, on behalf of the user, accesses classified data and files as required. For this situation to be analogous to the paper environment, the user program must be trusted not to downgrade any classified information to which it has access. For a program to be designated as trusted, it must be verified to act in a specified manner; in actual practice, the necessity to insure the correctness of a trusted program results in all but a few programs being designated as non-trusted. Consequently, in the ADP environment, special precautions must be implemented to insure that a non-trusted subject cannot purposely or inadvertently transfer information of one classification to a lower classification.

In addition to a security clearance, a person must have a need for access to the particular classified information or material in connection with the performance of his official duties or contractual obligations. In the paper environment, this restriction is implemented through the use of "need-to-know" controls. In an ADP system, this restriction is referred to as discretionary control. Discretionary controls implement a protection policy that may be dynamically defined by the user, and they correspond directly with the manual need-to-know controls. Non-discretionary controls implement a protection policy that, once defined for an object, is unchangeable and must be satisfied at all times. The policy addressing protection of national security information based on a person's clearance and the information's classification is a non-discretionary security policy.

In ADP systems, the problem is that of providing the necessary controls to satisfy the security policy, while, at the same time, allowing the most efficient use of computer resources by persons desiring to process data of various security classifications.

CURRENT ADP SECURITY PRACTICE

Most current ADP systems use special procedures for processing classified information. These procedures normally either permit only one security level of information to be processed at a time, or require that all users be cleared to the highest level in the system. Such an ADP system is housed in a facility cleared for the highest security level processed, and access is restricted to appropriately cleared individuals. If remote users must be supported by the ADP system, the personnel at the remote sites must also be cleared and their terminals housed in secure areas. The remote terminals and central facility must be linked by encrypted or protected communications circuits.

The two alternatives for processing several levels of classified information in ADP systems where adequate multilevel security protection is unavailable are system-high operation and dedicated operation. These terms are defined below:

- o System-High Operation - All security levels may be processed together, provided that all users and terminal areas are cleared for the highest level of information that could be processed on the system. All output from a system-high computer must be considered at the system-high level until it has been manually reviewed.
- o Dedicated Operation - Each level may be processed at a separate time, in which case the entire system environment must be changed or sanitized at each change of security level.

System-high operation requires an unnecessary profusion of personnel clearances, secure terminal areas, and secure communications. The dedicated operation requires that a procedure called "color-changing" be carried out when switching between different security levels. Dedicated operation allows uncleared terminals to be connected provided they are detached before classified processing begins; however, each change of environment wastes a significant amount of system time while sanitization is being completed. In either case, system-high or dedicated operation, the processing of multiple levels of classified information involves increased cost, inconvenience, and system inefficiency.

COMPUTER SECURITY REQUIREMENTS

It is clear that major problems have been encountered with the use of current ADP practices for processing multiple classifications

of information, especially in the areas of system costs and operational capabilities.

Cost Impacts

The cost impacts of computer security have been reflected in expenditures for increased protection, additional equipment, and inefficient system utilization. Additional personnel clearances, vault areas, and secure communications may be required to allow users to do unclassified processing on computers that handle classified data. For example, at the Air Force Data Services Center (AFDSC), the cost of securing each remote site was estimated at \$50,000.

Computer installations operating in a system-high mode that must provide responsive support to user communities of various clearance levels have had to purchase additional equipment. At AFDSC, a timesharing system was acquired to provide unclassified computing services to users in open office areas, supplementing the classified processing systems supporting users in secure terminal areas. In other cases, additional computers have been purchased to provide support to both classified and unclassified users.

Inefficient system utilization results when a system must be switched from processing at one classified level to another level. This switching, known as "color changing", requires that all processing of one security level be completed, system memories cleared, and a new version of the system be brought up before processing at another level can begin. The time required to perform the color change and restart the system ranges from twenty to forty-five minutes. The color change's effect may be propagated over one to two hours of processing time by refusing long jobs and saving files on backup tapes. Color changes are used in cases where responsiveness and workload do not require dedication of a computer to a given level for an indefinite period. Such changes can use ten to twenty percent of a system's processing capacity.

Operational Impacts

Operational requirements for secure computers have been met, when possible, by the two methods previously discussed: using a separate computer for each level, or clearing all users to the highest level being processed. These methods, however, do not satisfy the classified processing needs of some cases, such as when only a small portion of the data is classified or when the rapid transfer of information is required between operational forces.

In the first case, where a small portion of the data is classified, manual processing must be done on such data so that it is

not necessary to operate a system at the higher classification. Clearly, the operational impact of any delays resulting from the manual processing could be considerable, especially when rapid response to a developing situation is critical.

The second case, the transfer of information between operational forces, is exemplified by the difficulty in integrating intelligence and operational data. Such integration is required for responsive force management, but it must be done so as not to jeopardize intelligence sources. Since it is often impossible to clear all system users for the intelligence data, manual intervention is used: a cleared intelligence officer hands a subset of the data to the operations element. However, as automated, timely integration of such data becomes necessary, manual handling becomes unacceptable, and a direct technological solution to the problem of handling multiple classifications of information in an ADP system becomes necessary.

MULTILEVEL SECURITY IN ADP SYSTEMS

The economic and operational considerations previously discussed point to the need for developing the ability to process an arbitrary mix of classified and unclassified information simultaneously with a single computer, serving cleared and uncleared users, and relying on the computer's and operating system's internal controls to enforce security and need-to-know requirements. Such a computer would be operating in a true multilevel security mode. Two types of multilevel secure operation are: controlled--this operation would support users of different classifications, although all users would be cleared to some minimum level (e.g., a system with support for Secret and Top Secret users); open--this operation would support both cleared users and uncleared users (or users at unsecured terminals).

The costly procedures currently used are made necessary by the inability of the current hardware/software systems to protect the information they process. In a current ADP system, it must be assumed that any program that runs on the system can access any information physically accessible to the processor, and can retrieve, alter, or destroy the information as the programmer wishes. A number of projects have been undertaken to write programs that obtain access to information without authorization; in each case, total success was achieved.

Attempts to modify existing operating systems to remove security flaws have not been successful. Such ad hoc repairs, in many cases, may render the computer system inoperative unless a long and costly series of program modifications is made. In addition, complex program

changes, intended to correct security flaws, may introduce new flaws into other program areas.

The concept of program completeness is fundamental in the field of multilevel computer security. Even if every known security flaw in an operating system is corrected, the final operating system could not be considered secure, since successful system penetrations only show the existence of flaws, not the lack of them. While perfect security is not required in some areas (e.g., physical and personnel), the problem in computer security is not analogous to those in other areas. While flaws in physical security, for example, may permit unauthorized access a small percentage of the time, an operating system security flaw, which allows compromise of information, can be exploited at will, providing undetected access to any information in the computer. Given that a program can and would be written to capitalize on such a flaw, complete and unauthorized access could occur indefinitely. Strict security controls during design and production may prevent malicious code from being purposely inserted; however, unless security is a design consideration, the resulting system may contain design flaws that could provide access to unauthorized users.

This discussion shows that the method of correcting security flaws as they are found in a system cannot produce a secure system. The alternative is to develop a technical approach that results in a system to support classified processing in a true multilevel secure mode.

TECHNICAL APPROACH TO MULTILEVEL SECURITY

In 1970, the Air Force Data Services Center (AFDSC) asked the Electronic Systems Division (ESD) to support development of open multilevel secure operations for AFDSC's Honeywell 635 computer systems. ESD and MITRE personnel shortly reached the conclusion that no set of modifications to the 635's operating system would make it suitable for controlled multilevel operation, much less for open multilevel operation with uncleared users and terminals.

To determine the reasons for this difficulty, and to identify ways of solving future multilevel security problems, the Air Staff directed ESD in 1972 to convene a computer security technology planning study panel. The panel was composed of recognized experts from industry, universities, and government organizations and operated under a contract from ESD to James P. Anderson and Company. It was tasked with preparing a development plan for a coherent approach to attacking the problems of multilevel computer security. The panel was supported by a requirements working group of computer system staff officers from ten Air Force commands.

The panel's report (2) identified the problem of completeness and recognized the futility of "patching holes" in existing operating systems as a means of providing multilevel security. It recommended a technical approach that starts with a model of a secure system and refines it through various levels of design into hardware/software mechanisms that implement the model.

Reference Monitor

The basic component of the technical approach proposed by the security technology panel is the reference monitor: an abstract mechanism that controls access by subjects (active system elements) to objects (repositories of information) within the computer system. Figure 1 diagrams the relationships among subjects, objects, reference monitor, and reference monitor data base. An implementation of the reference monitor abstraction permits or prevents access by subjects to objects, making its decisions on the basis of information contained in the reference monitor data base. The implementation automates the access rules of the military security system and assures that they are enforced within the computer. The technology panel stated that, to be the basis for a multilevel secure computer system, a protection mechanism that implements a reference monitor must meet three requirements:

- o Complete mediation - the protection mechanism must be invoked on every access by a subject to an object.
- o Isolation - the protection mechanism and its data base must be protected from unauthorized alteration.
- o Verifiability - the protection mechanism must be small and simple enough so that it can be verified to perform its function correctly.

These requirements, and the need for efficiency, demand that the reference monitor implementation include hardware as well as software, since software validation of every access would add intolerable complexity and overhead to the reference monitor. Hardware features considered essential to implementation of a secure system include segmented memories, processors with multiple execution states, and positive control of all I/O devices.

The hardware/software protection mechanism that implements the reference monitor abstraction is called the security kernel. The software that must be designed to implement the reference monitor abstraction on a particular computer is frequently referred to as the security kernel for that computer.

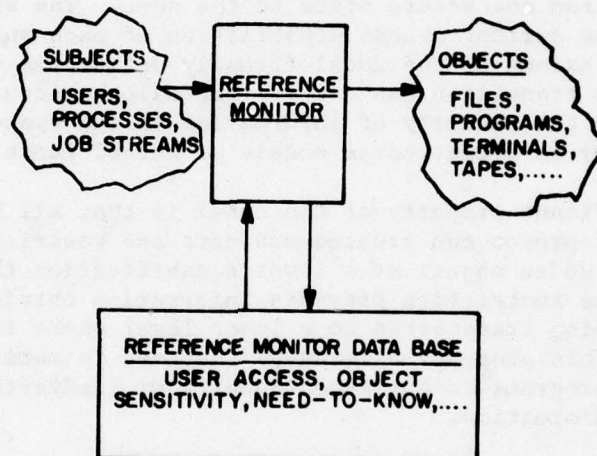


Figure 1. REFERENCE MONITOR

Abstract Model of a Secure System

Recognizing the importance of the model of an ideal system as a starting point, ESD initiated development of a mathematical model of computer security in 1972. Initial contributions were made by The MITRE Corporation (3) and by Case Western Reserve University (4,5). The model specifies the requirements for the operation of a security kernel. The basic requirements identified by the model are taken directly from Defense Department policy on handling sensitive information.

The completed model of secure computer systems represents a secure computer system as a finite-state mechanism that makes explicit transitions from one secure state to the next. The system state is defined by the current access capabilities of each subject to each object. The axioms of the model formally define the conditions under which a state transition can occur. The axioms allow only transitions that preserve the security of information in the system. Transition rules also may be suggested as models of kernel functions.

A significant property of the model is that all but a special collection of proven and trusted subjects are restricted from having write access to an object at a lower classification than any that it may read. The restriction prevents information obtained at the higher level from being transferred to a lower level where it can be accessed illegally. This property eliminates the need to verify that all non-trusted programs do not intentionally or inadvertently downgrade classified information.

Formal Specification

The mathematical model deals with abstract entities that must be realized in a concrete fashion. The first step in the process of realizing the model abstractions is to impose finite resource limitations on the abstract entities of the model and express the resulting system as a formal specification. This specification completely identifies the state variables of the representation and all the functions that a user might invoke to observe or modify one of these state variables. In the realization of any system based on the model, the objects must be given certain attributes such as type and size. Object type and size then become state variables, and functions must be provided in the formal specification to observe and manipulate these variables.

Algorithmic Representation

The functions of the formal specification must eventually be implemented by a set of algorithms, or programs. Since the formal

specification has decomposed the system into a series of function modules, the implementation of each module into a suitable high-level language follows the specification directly. The programs must then be proven correct with respect to a series of assertions, derivable from the formal specification.

Machine Language Representation

The programs developed from the formal specification will eventually be translated from a high-level language into a binary machine language, to run on a particular machine. It must then be shown that the resulting machine language corresponds directly with the high-level language representation.

Verification Techniques

Verification of the security software requires that the following five correspondences be shown to be correct:

- o Top level specification to model;
- o High-order language specification to top level specification;
- o High-order language code to high-order language specification;
- o Machine language to high-order language code; and
- o Microcode to machine language.

Top Level Specification to Model

All state variables in the formal specification are regarded as objects. The accesses to them are shown to satisfy the requirements expressed in the model.

High-Order Language Specification to Top Level Specification

Once the top level specification is completed, the correspondence between the top level specification and a software level specification must be shown. A methodology for showing this correspondence has been developed by the Stanford Research Institute (6); in this methodology, a hierarchical approach is used to design the software in such a way that the proofs required will be divided naturally into simple steps.

High-Order Language Code to High-Order Language Specification

The correspondence of the high-order language code to the high-order language specification can be shown through the use of a

methodology introduced by Floyd (7). The code level specification for a function plus the code relations provide the input and output assertions required by the Floyd technique. Automatic program verification tools will most likely need to be employed at this level to produce a rigorous and credible proof.

Machine Language to High-Order Language Code

There are two general approaches to the problem of proving that a machine language translation corresponds to a high-level language representation: use of a certified compiler, and use of an uncertified compiler and a certified disassembler.

The first approach establishes that the compiler being used generates semantically correct machine language code for any source program. Without the availability of certified compilers, one is faced with writing a compiler for a restricted subset of the implementation language and certifying that it compiles correctly.

The second approach is to compile the program into machine language and then to disassemble the resulting machine language into readable assembly language. The correspondence of the machine language program to the assembly language program would be assured by the certification of the disassembler. The correspondence of the assembly language program to the original program would be established manually. In this case, the overall correspondence of the high-level language to the machine language is shown by the composition of two smaller correspondences.

Microcode to Machine Language

When the instruction set of the machine is to be microprogrammed, attention should also be given to the correctness of the microcode.

Summary

The above techniques have been successfully used to provide multilevel security in computer systems. In addition, system procurements are underway that specify the use of these multilevel security techniques for providing computer security within the system. In the following subsections, examples of systems that have used or are planning to use these techniques are presented.

EXPERIENCES IN SECURE COMPUTER SYSTEMS

The following paragraphs present an overview of major secure computer system developments that apply hardware/software controls for the enforcement of security policy. The purpose of these examples is to demonstrate that security policy enforcement can be achieved through multilevel secure ADP systems, and to exhibit developing systems that employ this technology.

ESD/MITRE PDP-11/45 Security Kernel

To demonstrate the viability of the security kernel technology, ESD directed MITRE in January 1973 to begin implementing a prototype security kernel for the Digital Equipment Corporation PDP-11/45, a relatively large, moderately priced minicomputer. This kernel was initially intended to serve as the base for a front-end communications processor for use with a secure general-purpose computer system to be developed later; however, it was soon realized that the kernel could also support stand-alone secure computer applications requiring only a minicomputer, and it could serve to prove out the concept of a model and its implementation in a security kernel long before developing a kernel for a large general-purpose system. The ESD/MITRE PDP-11/45 kernel design provides a sound security foundation on which to base operating systems and applications programs that will function in a secure environment (8).

The ESD/MITRE kernel design for the PDP-11/45 was developed by applying levels of abstraction to separate those parts of the kernel that implement the security rules, objects, and subjects required by the model. The kernel implements separate sequential processes that can cooperate and communicate in accordance with the rules of the model. This kernel design creates a very basic secure environment upon which operating systems and application programs can be implemented. The access of users (subjects) to information (objects) in such a kernel-based system conforms to the specified security rules since all system and applications software is running on top of the security kernel.

As a practical demonstration of security kernel technology, a MITRE project built a secure, multilevel file management system on the PDP-11/45 kernel. Two scenarios using this file system have been developed (9). The first of these scenarios uses a text editing capability to show how a multilevel data base can provide for data storage, manipulation, and retrieval in a multilevel user environment, while protecting all classified information from unauthorized access. The second demonstration employs an air surveillance data correlation

scenario that permits precisely controlled, selective downgrading of classified track data based on the informed judgment of a downgrading officer. The system being demonstrated allows users to access the widest possible range of information on the system (restricted only by their maximum clearances), yet prevents the unauthorized user from accessing any classified information not specifically downgraded.

The PDP-11/45 kernel design is implemented in a small structured computer program and follows the mathematical model directly. This PDP-11/45 security kernel provides a demonstration of the feasibility of building a security kernel that implements a security policy model.

AFDSC Secure Multics

While the security kernel for the PDP-11/45 constitutes a small secure system, Air Force commands need large multilevel secure computers. The reference monitor concept must be demonstrated to be feasible in an efficient, as well as secure, large resource-sharing system. This demonstration is necessary to show that systems based on the reference monitor concept can provide a viable solution to meeting all Air Force ADP requirements (not just those for security).

Initial steps toward developing a secure system based on Multics were taken in conjunction with development of a Multics operating system for use in a two-level (Secret and Top Secret) environment at the Air Force Data Services Center. This system's design is aimed at providing security controls based on the military access rules, but it does not attempt to eliminate completely the prospect of hostile penetration. The risk of penetration is to be reduced primarily by procedures and by personnel and environmental controls, rather than by the Multics hardware and software. The implementation of the access rules in the Data Services Center Multics was based on the concept of a secure system model, but no attempt was made to define a security kernel for the system.

Honeywell Information Systems began the design of the Data Services Center Multics in late 1973, and it was completed in mid-1974 (10). Implementation was completed in 1975 and the system is currently in operation. As noted, the system was designed for use in a controlled environment where all users are cleared to either the Secret or Top Secret level. Because of this benign environment, a kernel-based design was not required for certification. This system was the first operational system to be certified for multilevel computation in DoD. The system was approved for simultaneous servicing of both Secret and Top Secret cleared personnel by the Commander, Air Force Data Automation Agency, on 2 December 1976.

SATIN IV

SATIN IV, the Strategic Air Command (SAC) Automated Total Information Network, is a packet-switched network that will support the World Wide Record/Data Command Control Communications requirements of SAC and the National Command Authorities. Due to the sensitive nature of the SATIN IV message traffic, security has been identified as a major design requirement. An Internal Access Control Mechanism (IACH) will be used in the SATIN IV communications processors to provide security to messages at each of the SAC base locations. This IACH, augmented by a number of trusted processes, draws heavily on previous computer security technology work.

AUTODIN-II

AUTODIN-II is a packet-switched network to be developed for the Defense Communications Agency (DCA). Its aim is to provide a common Department of Defense communications system for computer-to-computer and terminal-to-computer connections. The Initial Operating Capability, which includes three packet switching nodes (PSNs) and a Network Control Center, is scheduled for early 1979.

As with SATIN IV, a security kernel (referred to as a System Security Module) will be developed for use in the PSNs to implement the requirements of DoD security policy. The System Security Model is intended to provide the necessary security for messages as they travel throughout the AUTODIN-II network.

Secure UNIX Procurement

Prototype Secure UNIX efforts have been undertaken at MITRE and UCLA. Under USAF/ESD sponsorship, MITRE is implementing a prototype Secure UNIX kernel on a PDP-11/45. The kernel is a new version of the original 11/45 kernel developed at MITRE, and it is largely coded in the Bell Laboratories C language, as is the program that establishes the UNIX interface. The interface program, called the Secure UNIX Emulator, uses the kernel-supplied functions and provides other needed functions to duplicate, as nearly as possible, the user program interface provided by commercial UNIX.

An ARPA-sponsored effort at UCLA is producing a kernel-based UNIX system of different design from the ESD/MITRE system. While the UCLA kernel creates processes having a per-process virtual environment, as does the MITRE kernel, the specific kernel implementation is different. The kernel provides for process creation and control, page control and swapping, and provides for I/O and interprocess communication capabilities. The UCLA kernel offers another design approach to the construction of a Secure UNIX.

An ARPA-sponsored procurement is underway to develop a production version of a secure operating system that can be used in a wide variety of DoD applications. The results of this procurement will be a secure system based on the security kernel technology, and offering the features of the UNIX operating system. UNIX is a general-purpose timesharing system that operates on the Digital Equipment Corporation PDP-11 series computer. The UNIX system was designed to provide a good environment for the user to develop and operate information processing and computational systems. UNIX is of interest to DCA (as a WWMCCS network front-end), to the Air Force Data Services Center (for text processing and intercomputer interfacing), and to the intelligence community (for several stand-alone and network applications). These UNIX applications would, without exception, be facilitated if they could be implemented on a secure version of UNIX capable of enforcing the DoD security policy.

There are six major objectives of the Secure UNIX procurement:

- o The resulting system shall be verifiably secure with respect to DoD policy.
- o The resulting system shall provide adequate performance.
- o The resulting system shall allow applications programs written for unsecure UNIX to be run without modification, provided the program is only required to process a single level of information.
- o The resulting system shall include administrative and user interface functions to facilitate the processing of DoD classified information in a true multilevel environment.
- o The resulting system shall support a single-level interface to the ARPANET, and shall allow for the incorporation of evolving multilevel network security protocols.
- o The resulting system shall be fully documented to allow for wide use, maintenance, and enhancement within the DoD community.

Work on the Secure UNIX development began in August 1977 with TRW and the Ford Aerospace and Communications Corporation as contractors. Implementation of Secure UNIX should be completed by September 1979.

SUMMARY OF REQUIREMENTS

Based on the discussion in this section, a number of requirements must be met to provide a true multilevel secure computer system; it is imperative that the appropriate DoD directives adequately address the need for these features. The features are summarized below.

A complete and provably secure representation of the protection mechanism based on the abstract security model is needed to evaluate the adequacy of the protection mechanism. This formal representation embodies the constraints imposed on information access by the security policy. A protection mechanism that is built based on such a representation can be checked for adequacy through the following three steps:

- o Validation - technical proof that security policy is enforced.
- o Certification - application of technical and procedural measures to a system to a degree commensurate with the threats perceived in the system environment.
- o Accreditation - official approval of a system issued by the appropriate authority.

Such a protection mechanism must enforce the two properties dictated by the security policy. These properties are:

- o General Access Property - A subject will be allowed to read an object only if the classification level of the subject is greater than or equal to the classification level of the object, and the subject is authorized access to the set of categories that are assigned to the information.
- o Special Access Property - A non-trusted subject will not have read access to an object of a higher classification or possessing a more restrictive set of categories than an object to which the subject concurrently has write access, i.e., information from an object with a given classification and set of categories may only be transferred into an object with an equal or higher classification and category.

After a protection mechanism is developed that satisfies the two properties described above, it is still necessary to assess the overall security of the ADP system based on the incorporation of the mechanism into the system. Such an assessment can be accomplished in

a security test and evaluation (ST&E) procedure, performed by technical and security personnel, whereby:

- o the vulnerability threats are identified;
- o effective countermeasures are determined;
- o the countermeasures are implemented in compliance with the appropriate security directives and procedures for the different classifications handled; and,
- o despite any unresolved security risks, the system still provides an adequate degree of security.

While this ST&E procedure does not in itself guarantee that an ADP system is secure, it is a step required to determine the overall system's ability to provide the security dictated in DoD policy.

In addition to the above development of a protection mechanism and the evaluation of the security of an ADP system, strict controls are needed during design and production of the system, since a protection mechanism will be of little value if unauthorized code (e.g., a trap door or trojan horse program) is inserted during system construction.

Thus, the directives must dictate that at least the following criteria be satisfied to insure that security policy requirements are met and that security policy is enforced:

- o The general access and special access properties must be adhered to for every read or write operation within the system.
- o No system software shall be put in operation until it has been suitably verified, certified, and accredited for general use by the proper approving authorities.
- o Security test and evaluation procedures must be used to determine the overall system's ability to enforce DoD security policy.
- o Controls must be implemented during all stages of design and production to insure that no disruptive code is inserted into the system procedures.

The next section examines the directives in light of these necessary criteria.

SECTION III

ADDITIONS AND MODIFICATIONS TO EXISTING DIRECTIVES

The previous section discussed security policy in ADP systems, and how the problem of providing a true multilevel secure environment is being addressed. As shown, systems exist and are being developed to handle all classification levels of information simultaneously within a computer system. Based on those developments, this section examines three existing directives (DoD 5200.28, DoD 5200.28M, and AFR 300-8) to determine what additions and modifications are necessary to reflect this availability of multilevel secure computer technology. In particular, the areas summarized at the end of the previous section will be considered for this set of directives. A general discussion of the additions and modifications is followed by specific discussion for each directive.

GENERAL

One main area where the directives lack completeness is in specifying the application of design and production controls. Adequate controls are necessary during the design and production cycles of an ADP system to insure that devices and programs that might be used to compromise classified information during system operation cannot be inserted without detection. The directives must explicitly state the need for adequate controls during design and production.

The directives must also state more clearly the need for certified dependability in implementing the security controls; in addition, the responsibility and authority for accrediting a system must be identified.

DOD DIRECTIVE 5200.28

DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems", presents the security requirements that must be adhered to when implementing an ADP system. As currently written, this directive is not sufficiently definitive on the extent of dependability that the ADP security procedures must maintain. When considering the simultaneous processing of information of different classification levels, it is clear that a system must be certain to incorporate proper safeguards to prevent undetected security violations. The state-of-the-art in computer security is such that these safeguards can be achieved. Consequently, the directive should

require that any ADP security procedures are shown to be certified for protecting all classified information. This certification requirement is needed as an assurance that the system upholds the security policy.

Since present ADP security technology has developed mainly in the time after this directive was issued, the directive does not address security properties that have been identified as peculiar to the ADP environment. Although the general access property is covered to the extent that protection against compromise is required, the special access property is not addressed. This property, and the requirement that security protection mechanisms support it, must be incorporated into the directive. In addition, suitable mechanisms must be provided in a system to handle the enforcement of discretionary and non-discretionary controls.

This directive restricts contractor processing of classified information to systems that are operated in the dedicated mode; however, with the development of secure multilevel systems, this restriction could be eased to allow contractor processing of classified material on either a dedicated system or a system that has been certified as multilevel secure.

Any ADP system that will be processing classified information must meet the security requirements set forth in this directive. While verification and certification procedures can show that the system is secure, some authority must accredit these findings and declare the system suitable for operational use. This accrediting authority has not been identified within the directive and must be included.

The minimum requirements for effective security, as set forth in the directive, must be expanded to cover design and production controls. As the previous section showed, security during these stages of system development is critical to the ultimate system operational security.

DOD MANUAL 5200.28M

DoD Manual 5200.28M, "Manual of Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems", discusses methods available to implement an ADP system that satisfies the requirements set forth in DoD 5200.28. As in DoD 5200.28, this manual should be modified to be more definite regarding the extent of dependability that must be maintained by ADP security procedures. The manual should require certified dependability for ADP systems handling classified material, rather than simply "reasonable dependability".

While clearance and access controls are discussed within the manual, these controls must be made more specific for the design and production phases of system development. As currently written, these controls apply only to operating system programming personnel, and seem to be applicable mainly to programming occurring after system installation. A separate paragraph in Section II of the manual should clearly detail the clearance and access control requirements during design and production.

This manual discusses the application of a combination of hardware and software features to provide protection to classified information in ADP systems. In this regard, the concept of a reference monitor and the security kernel as an implementation of the reference monitor, for mediating all accesses of subjects to objects, should be included. This additional information could be added to the discussion of hardware/software features in Section IV.

The description of the hardware features in Section IV of the manual can be expanded in light of the minimum hardware requirements that have been identified as necessary to support secure ADP software. As presently worded, this section deals mainly with control of processor actions, e.g., error detection on memory fetches and known responses by all operation codes. In addition to hardware features such as these, other features to provide isolation of the security kernel and the ability to manipulate subject and object access attributes must exist in a secure system. Although implied in the hardware discussion, the necessity for multiple execution domains and segmented memory, or equivalent capabilities, in the processor must be explicitly noted.

This manual states that the operating system shall contain controls that provide the user with all material to which he is authorized and no more. As noted, such controls could be implemented through the use of a security kernel implementation of a reference monitor that mediates all access of subjects (users or user processes) to objects (data material). Since the security kernel provides the security needed in the operating system, this technique satisfies the requirements of the manual. As presently written, the manual does not make it clear that the use of security kernel technology is a feasible and acceptable solution to implementing security controls.

The Security Testing and Evaluations section can be expanded to include not only the need for validating, certifying, and accrediting the security measures used for a given ADP system, but how these evaluations can be accomplished.

Auditing and surveillance can provide feedback on how users are employing the ADP system. Such techniques augment the security controls of the ADP system. While existing manuals require that records be kept of logins, file creations, file accesses, and classified outputs, it is equally important that attempts to circumvent the security rules be recorded as well. In addition, changes to system status should be recorded so that an accurate history of system operation can be maintained. Additional items to be recorded would include: failures of logins, file accesses, file creations, or classified output attempts; changes to access privileges; changes to directories; downgrading attempts; hardware failures; and, system crashes. The system security officer should be provided with the capability to monitor security-related events while in progress, as a means of detecting violations as they occur. The extent to which these auditing and surveillance features would be incorporated into an ADP system would depend on the requirements of the specific ADP system.

AIR FORCE REGULATION 300-8

Air Force Regulation 300-8, "Security Requirements for Automatic Data Processing Systems (ADPS)", establishes policy and assigns responsibilities for the implementation of ADP security procedures in Air Force systems. This regulation presents the Air Force-specific amplifications to the security requirements and procedures put forth in DoD 5200.28 and 5200.28M.

For any system, a model must be developed, incorporating the minimum requirements; such a model can be used for comparison to the actual system and determining the adherence to the minimum requirements. This regulation must incorporate the concept of developing a model as a means of checking a system and its security procedures.

As in the previous two cases, this regulation does not fully explain the requirements for design and production controls during system development. The regulation does state that the application of design and production controls during system development must be assured; however, details on these design and production requirements, and the responsibility for setting these requirements, are lacking. An additional paragraph must be added to the "Minimum Requirements" section to expand on the requirement for adequate security controls during design and production. In the responsibilities section, the responsibility to set the requirements of design and production controls must be added to the stated responsibilities for such areas as security approval procedures and approval of ADP systems to handle classified material.

The "Minimum Requirements" outlined in this regulation should be reflected in the model used to analyze the final system configuration. Consequently, this regulation must include the requirement that the model incorporate the minimum requirements as presented.

SECTION IV

CONCLUSIONS AND RECOMMENDATIONS

It is clear from the discussion in this paper that existing DoD ADP system directives need to be updated to reflect the new developments in computer security technology. As mentioned in the Introduction, the directives recognize the need for updating when new developments in ADP system security are available. With security kernel technology now being used and being planned for use in a number of systems, the fact that new developments are available becomes apparent.

It is recommended that these three directives (DoD 5200.28, DoD 5200.28M, and AFR 300-8) be suitably revised to reflect the state-of-the-art in computer security technology. This paper has identified the major areas of revision, and appropriate changes have been suggested.

It has been recognized that security cannot be "added-on" to a design. Many DoD directives influence the hardware and software design cycle. While specific changes are recommended for the above three directives, a general security awareness in all system design and operations directives also is needed.

APPENDIX I

PROPOSED CHANGES TO DOD 5200.28

This appendix presents specific word changes that would modify DoD 5200.28 to reflect the suggested additions and modifications discussed in Section III.

SECTION I - PURPOSE

Part B3 currently states that systems that handle classified information will, "with reasonable dependability", prevent unauthorized access or modification. The phrase, "with reasonable dependability", should be changed to reflect the addition of certification requirements into subsequent sections. Two alternate phrases are: "with dependability", or "with certified dependability".

SECTION III - DEFINITIONS

Any additional computer security terms used in these changes must be added to the definition list included as Enclosure 2. (See additions to Enclosure 2 - Definitions.)

SECTION IV - POLICY

Part A states that each DoD component shall assure adherence to the policies. This part could be changed to include a certification requirement (e.g., each DoD component shall certify...); the certifying authority is described in a later part.

A new part should be added to this section to detail the requirement to satisfy the general access and special access properties, and, in addition, the requirement to provide discretionary and non-discretionary controls. This new part would read as follows: "The security measures for ADP systems operating in a true multilevel secure mode shall be implemented to enforce both the general access and special access properties, and to provide discretionary and non-discretionary controls."

In Part O, the handling of Top Secret information by a contractor ADP system is restricted to system operating in a dedicated mode. This restriction could be modified to include the alternative of

introducing Top Secret information to a contractor ADP system that has been "certified as multilevel secure by a cognizant DoD authority."

SECTION V - RESPONSIBILITIES

To the responsibilities of the DoD component Designated Approving Authority (Part C), the accreditation authority must be added. This authority will decide if the system is acceptable, based on the findings of the certification authority.

SECTION VI - MINIMUM REQUIREMENTS

A new part should be included on "Design and Production Controls". This part would deal with software development in a classified environment. The new part would be as follows: "8. Design and Production Controls. Adequate security controls shall be provided to assure that the system security controls are protected from subversion during system design and production."

ENCLOSURE 2 - DEFINITIONS

The following definitions should be added to Enclosure 2:

Discretionary Controls - a protection policy that may be dynamically defined by the user.

Non-Discretionary Controls - a protection policy that, once defined for an object, is unchangeable and must be satisfied for all states of the system.

General Access Property - A subject will be allowed to read an object only if the classification level of the subject is greater than or equal to the classification level of the object, and the subject is authorized access to the set of categories that are assigned to the information.

Special Access Property - A non-trusted subject will not have read access to an object of a higher classification or possessing a more restrictive set of categories than an object to which the subject concurrently has write access.

APPENDIX II

PROPOSED CHANGES TO DOD 5200.28M

This appendix presents specific word changes that would modify DoD 5200.23M to reflect the suggested additions and modifications discussed in Section II.

SECTION I - GENERAL PROVISIONS

Part 1 - Introduction

The objective should be modified along the lines of the DoD 5200.28 changes, such as including the term "certified dependability". The responsibilities outlined in this part must include the certification and accreditation authority designations.

SECTION II - PERSONNEL SECURITY

Part 1 - Clearance and Access Controls

Although this part mentions the need for the proper clearance of ADP personnel, additional information must be included on the clearance and access controls during design and production. This additional information could be included as a new paragraph within this part, or the design controls mentioned in paragraph 2-102, Operation and Operating System (O/S) Programming Personnel, could be made more explicit.

SECTION IV - HARDWARE/SOFTWARE FEATURES

Part 1 - General

This part discusses the use of a combination of hardware and software to provide the ADP security protection. This part can be expanded to include additional background information dealing with the reference monitor and security kernel concepts. The major point to be included is that "the concept of a reference monitor and the security kernel as an implementation of the reference monitor, for mediating all accesses of subjects (processes) to objects (data or files), is an example of a technique to provide protection for material stored or processed in secure ADP systems."

Part 2 - Hardware

The following paragraph would identify additional hardware features necessary in secure ADP systems:

"Additional hardware features must be included to provide isolation of the protection mechanism and to provide the ability to manipulate subject and object access attributes."

Part 3 - Software

The reference monitor and security kernel concepts should be incorporated into Paragraph 4-301 - O/S Controls. The following sentence could be added: "Such controls could be implemented through the use of a security kernel implementation of a reference monitor that mediates all accesses of subjects to objects."

SECTION IX - SECURITY TESTING AND EVALUATIONS (ST&E)

The goals of the ST&E procedures could be added to this section using the following paragraph:

"To assess the overall security of the ADP system with a procedure whereby:

- the vulnerability threats are identified;
- effective countermeasures are determined;
- the countermeasures are implemented in compliance with the appropriate security directives and procedures for the different classifications handled; and
- despite any unresolved security risks, the system still provides an adequate degree of security."

APPENDIX III

PROPOSED CHANGES TO AFR 300-8

This appendix presents specific word changes that would modify AFR 300-8 to reflect the suggested additions and modifications discussed in Section III.

PART 3 - PARAGRAPH C

The need for a complete and provably secure representation of the protection mechanism should be incorporated into this part. Following the discussion of the need for comprehensive testing, this sentence should be added: "A complete and provably secure representation of the protection mechanism used in the system must be developed for use in determining the adherence of the system to the minimum requirements of this regulation."

PART 4 - INTRODUCTION

In the introduction to this part, words should be added that explain the need for the system's protection mechanism to reflect the minimum requirements as set forth in this part. After the discussion of the initial testing and evaluation, the following should be added: "The protection mechanism that is developed for the ADP system must satisfy the minimum requirements for internal system security as set forth below."

PART 4 - PARAGRAPH H

A new paragraph should be added under "Minimum Requirements" to reflect the requirement for adequate controls during the design and production phases of system development. This paragraph expands upon the objective set forth in part 2.b(1) of the regulation. The paragraph would be as follows:

- "h. Design and Production Controls. Adequate controls are instituted to assure that the necessary system security controls are protected from subversion during system design and production."

PART 6 - PARAGRAPH A

A paragraph must be added to this part to identify the responsibility for setting the requirements of design and production controls. Since this responsibility is of a critical nature, it would most likely fall under the Office of Primary Responsibility. The additional paragraph would be as follows:

- "(7) Establishes the requirements for design and production controls necessary to assure the protection of security controls during these phases of system development."

REFERENCES

1. DoD 5200.1-R, "Information Security Program Regulation", 28 May 1975.
2. J. P. Anderson, "Computer Security Technology Planning Study", ESD-TR-73-51, Volumes I-II, James P. Anderson & Co., Fort Washington, Pennsylvania, October 1972.
3. D. E. Bell and L. J. LaPadula, "Secure Computer Systems", ESD-TR-73-278, Volumes I-III, Electronic Systems Division, AFSC, Hanscom AFB, Massachusetts, November 1973 - June 1974.
4. K. G. Walter, et al., "Primitive Models for Computer Security", ESD-TR-74-117, Case Western Reserve University, Cleveland, Ohio, January 1974.
5. K. G. Walter, et al., "Initial Structured Specification for an Uncompromisable Computer Security System", ESD-TR-75-82, Case Western Reserve University, Cleveland, Ohio, July 1975.
6. J. H. Spitzzen, K. N. Levitt, and L. Robinson, "An Example of Hierarchical Design and Proof", Technical Report 2, Stanford Research Institute, Menlo Park, California, March 1976.
7. R. W. Floyd, "Assigning Meaning to Programs", Mathematical Aspects of Computer Science, Volume 19, American Mathematical Society, Providence, Rhode Island, 1967, pp. 19-32.
8. W. L. Schiller, "The Design and Specification of a Security Kernel for the PDP-11/45", ESD-TR-75-69, Electronic Systems Division, AFSC, Hanscom AFB, Massachusetts, May 1975.
9. J. L. Mack and B. N. Wagner, "Secure Multilevel Data Base System: Demonstration Scenarios", ESD-TR-76-158, Electronic Systems Division, AFSC, Hanscom AFB, Massachusetts, June 1975.
10. J. C. Whitmore, et al., "Design for Multics Security Enhancements", ESD-TR-74-176, Honeywell Information Systems, December 1973.